COMPARTILHAMENTO DE DADOS PESSOAIS NO ÂMBITO DA ADMINISTRAÇÃO PÚBLICA: UMA ANÁLISE DA ADI 6.649 E DE SUAS REPERCUSSÕES NORMATIVAS

Marcela Gaspar Pedrazzoli[1]

RESUMO

O artigo realiza um estudo descritivo da Ação Direta de Inconstitucionalidade (ADI) n.º 6.649, na qual o Supremo Tribunal Federal julgou a constitucionalidade do Decreto Federal n.º 10.046, de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Nesse sentido, ancorando-se em uma análise indutiva e qualitativa dos documentos disponíveis nos autos digitais públicos da referida ADI, o trabalho expõe: (i) os argumentos aduzidos pelos atores envolvidos no julgamento; (ii) os argumentos centrais do voto vencedor; e (iii) as modificações introduzidas no Decreto Federal após a decisão da Corte Constitucional. Após esse percurso, o estudo conclui apontando os parâmetros que podem ser extraídos da decisão do STF e elucida os pontos que não foram plenamente equacionados no julgamento e tampouco na modificação normativa que lhe sucedeu.

PALAVRAS-CHAVE: Proteção de dados pessoais; autodeterminação informativa; compartilhamento de dados pessoais; Administração Pública Federal.

INTRODUÇÃO

Os avanços das ferramentas tecnológicas na área da informática – que têm como expressões o desenvolvimento de algoritmos e a computação em nuvem – trouxeram a possibilidade de coleta, armazenamento e processamento de dados em larga escala. Se, na perspectiva dos agentes privados, referidas inovações fomentaram o desenvolvimento de uma poderosa economia digital, marcada pela personalização de produtos, serviços e publicidade; sob o viés do Poder Público, tais inovações abriram o caminho para uma atuação mais eficiente do Estado, com políticas e serviços públicos orientados pela análise de dados e cada vez menos dependentes do uso do papel ou da presença física do cidadão nas repartições.

Uma das ferramentas de que dispõe a Administração Pública para buscar essa eficiência decorrente do processamento de dados é o compartilhamento de informações coletadas e armazenadas por determinado órgão público com outro. Com efeito, o compartilhamento de dados entre órgãos e entidades, além de permitir uma ampliação dos dados disponíveis para orientar a ação do Poder Público, pode ter como desdobramentos o afastamento da necessidade de que o cidadão forneça o mesmo

1 Procuradora do Estado de Mato Grosso do Sul, mestranda em Direito do Estado pela Faculdade de Direito da Universidade de São Paulo (FDUSP) e graduada pela FDUSP.

dado diversas vezes a distintos órgãos públicos, bem como o aprimoramento da qualidade dos dados disponíveis (já que o cruzamento de informações pode levar à identificação e à correção de eventuais inconsistências). Para melhor ilustrar essa afirmação, convém pontuar que, durante a pandemia da Covid-19 no Brasil, a identificação do público-alvo de benefícios sociais se materializou mediante o compartilhamento de dados entre órgãos e entidades da Administração, por meio de técnicas de interoperabilidade.[2]

Todavia, é preciso obtemperar que, se a ferramenta do compartilhamento for utilizada de forma indiscriminada e tiver como objeto dados pessoais – entendidos estes como as informações relacionadas à pessoa natural identificada ou identificável[3] –, ela tem o potencial violar direitos fundamentais, principalmente o direito à proteção de dados pessoais[4], recentemente positivado no artigo 5º, inciso LXXIX, da Constituição. Aliás, nos últimos anos, o Supremo Tribunal Federal (STF) apreciou diversas pretensões de compartilhamentos de dados entre instituições públicas que reputou como lesivas à Constituição[5].

Assim, é evidente que a definição de parâmetros para o compartilhamento de dados (especialmente os pessoais) entre órgãos e entidades da Administração Pública se revela essencial para o desejado alcance do equilíbrio entre, de um lado, a eficiência na gestão pública (artigo 37, *caput*, da Constituição) e, de outro, a adequada proteção de direitos fundamentais. E, em um contexto no qual a doutrina sobre esse tema ainda é escassa e a Lei Federal n.º 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) é pouco minudente[6], ganha relevo o estudo de casos concretos.

Nesse cenário, o presente artigo se propõe a realizar uma análise descritiva da Ação Direta de Inconstitucionalidade (ADI) n.º 6.649, na qual o STF julgou a constitucionalidade do Decreto Federal n.º 10.046, de 2019, que disciplina o compartilhamento de dados no âmbito da Administração federal. O objetivo é, essencialmente, descrever como se deu a dinâmica de impugnação, julgamento e alteração normativa, para, ao final: (i) apontar quais parâmetros podem ser extraídos da decisão do STF; e (ii) elucidar os pontos que não foram plenamente equacionados no julgamento e na modificação normativa, de modo a lançar bases para ulteriores propostas doutrinárias e legislativas de solução.

Para o alcance dessa finalidade, além desta Introdução, o artigo possui quatro partes. No Tópico 2, far-se-á uma breve explicação do conteúdo do Decreto Federal n.º 10.046, de 2019, na redação vigente quando de sua impugnação por meio da ADI 6.649. Em seguida, no Tópico 3, promover-se-á uma descrição dos principais argumentos levados ao Supremo para questionar e defender a constitucionalidade do Decreto, oportunidade em que se apresentará, também, o conteúdo do voto vencedor. De forma sistemática, no Tópico 4, serão expostas as modificações mais relevantes introduzidas no Decreto n.º 10.046, de 2019 após o julgamento. Por fim, o Tópico 5 abrange as considerações finais.

2 Conforme item 64 da Nota Técnica SEI n.º 5901/2020/ME, contida nos autos públicos da ADI 6.649, disponível no sítio eletrônico do STF: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238 (Acesso em: 04.12.2022).

3 A definição foi extraída do artigo 5º, inciso I, da Lei Geral de Proteção de Dados Pessoais (LGPD).

4 O conteúdo do direito à proteção de dados pessoais será explorado no Tópico 3.1., letra "a", deste artigo.

5 Nesse sentido: SL 1.103 MC, Rel. Min. Cármen Lúcia, julgado em 5.2.2017, DJe 8.5.2017 e MS 36.150 MC, Rel. Min. Roberto Barroso, julgado em 10.12.2018, DJe 13.12.2018.

6 WIMMER, Miriam. Limites e possibilidade para o uso secundário de dados no Poder Público: Lições da Pandemia. *In:* Revista Brasileira de Políticas Públicas. Vol. 11, n.º 1. Abr. 2021.

1. O CONTEÚDO ORIGINAL DO DECRETO

Para a adequada compreensão da controvérsia submetida à apreciação do Supremo Tribunal Federal, faz-se necessário, de início, conhecer, mesmo que forma perfunctória, o teor do Decreto Federal n.º 10.046, de 2019 quando de seu controle de constitucionalidade.

Nessa toada, esclarece-se que o âmbito de aplicação do Decreto é o compartilhamento de dados entre os órgãos e as entidades que compõem a Administração Pública Federal direta, autárquica e fundacional e os demais Poderes da União. E, mesmo nesta seara, foram expressamente excluídos os compartilhamentos que envolvam conselhos de fiscalização profissional, o setor privado e dados protegidos por sigilo fiscal sob a gestão da Secretaria Especial da Receita Federal.

Quanto ao conteúdo, o Decreto pode ser dividido, essencialmente, em *cinco* eixos. O *primeiro* refere-se às suas normas introdutórias, nas quais são definidos os objetivos do compartilhamento de dados no âmbito da Administração Pública Federal (artigo 1º), os conceitos empregados na normativa (artigo 2º), bem como as diretrizes para o compartilhamento (artigo 3º).

O *segundo* diz respeito às regras para o compartilhamento de dados (artigos 4º a 15), as quais se estruturam a partir de uma categorização em três níveis de compartilhamento, utilizando-se como critério a confidencialidade do dado. Registre-se que a atribuição de promover a aludida categorização é do gestor dos dados, sendo este último entendido como "o órgão ou entidade responsável pela governança de determinado conjunto de dados"[7]. E, ele deve fazê-lo com base na legislação.

Dito isso, importa explicar cada uma das categorias de compartilhamento. O "compartilhamento amplo" dá-se nos casos de dados públicos, não sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser garantida a qualquer interessado, dispensando-se autorização prévia pelo gestor dos dados. O "compartilhamento restrito", por sua vez, ocorre nos casos de dados protegidos por sigilo, cujo acesso é franqueado a todos os órgãos e entidades abrangidos pelo Decreto, para fins de execução de políticas públicas, cabendo ao Comitê Central de Governança de Dados (CCGD) – que será adiante descrito – estabelecer mecanismos e regras simplificadas de compartilhamento. Enfim, o "compartilhamento específico" dá-se nos casos de dados protegidos por sigilo, mas para os quais a concessão de acesso é franqueada tão somente a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei, cabendo ao gestor dos dados definir as regras e conceder permissão de acesso.

Observe-se, ademais, que, conforme o regramento da normativa, os solicitantes e recebedores dos dados devem assumir a responsabilidade por implementar e seguir as regras de sigilo e segurança estabelecidas pelo CCGD, pelo gestor de dados e/ou pelo gestor da plataforma de interoperabilidade, conforme o caso. Lado outro, aos gestores de dados cabe a divulgação dos mecanismos de compartilhamento de seus dados e dos cadastros base[8] sob sua responsabilidade.

Ainda no que tange às regras de compartilhamento, o Decreto dispensa a celebração de instrumentos cooperativos (acordos, convênios etc.) para a efetivação do compartilhamento de dados entre os

7 Cf. definição do artigo 2º, inciso XIII, do Decreto Federal n.º 10.046, de 2019.

8 Cf. definição do artigo 2º, inciso XXV, do Decreto Federal n.º 10.046, de 2019, o cadastro base consiste na "informação de referência, íntegra e precisa, centralizada ou descentralizada, oriunda de uma ou mais fontes, sobre elementos fundamentais para a prestação de serviços e para a gestão de políticas públicas, tais como pessoas, empresas, veículos, licenças e locais".

órgãos e entidades por ele abrangidos, observadas as diretrizes da própria normativa e a LGPD.

Prosseguindo, o *terceiro* eixo concerne à instituição do denominado "Cadastro Base do Cidadão" - CBC (artigos 16 a 20), o qual, entre outras finalidades, busca: viabilizar a criação de um meio unificado de identificação do cidadão para a prestação de serviços públicos; facilitar o compartilhamento de dados cadastrais do cidadão entre os órgãos da administração pública; e realizar o cruzamento de informações das bases de dados cadastrais oficiais a partir do número de inscrição do cidadão no Cadastro de Pessoa Física (CPF). Nessa direção, o CBC pode ser compreendido com um cadastro de dados apto a servir de referência de informações sobre os cidadãos para os órgãos e entidades do Poder Executivo federal.

Nos termos do Decreto, o CBC seria composto por uma base de dados integradora e por componentes de interoperabilidade, os quais possibilitariam o intercâmbio da referida base integradora com as bases de dados próprias de determinadas políticas públicas (chamadas de "bases temáticas"). Previu-se que, inicialmente, a base integradora seria disponibilizada com os dados biográficos que constam da base temática do CPF, aos quais, posteriormente, seriam acrescidos dados provenientes de outras bases, a partir do número de inscrição do CPF. A norma também prevê a realização de atualizações das bases temáticas, com envio periódico à base integradora.

O *quarto* eixo a ser mencionado versa sobre a instituição do Comitê Central de Governança de Dados (CCGD), já citado acima. Trata-se do órgão principal para a implementação do fluxo de compartilhamento instituído pelo Decreto, tendo em vista suas relevantes atribuições, dentre as quais merecem destaque as de deliberar sobre: orientações e diretrizes para a categorização de compartilhamento amplo, restrito e específico, e a forma e o meio de publicação dessa categorização, observada a legislação de proteção de dados pessoais; regras e parâmetros para o compartilhamento restrito, incluídos os padrões relativos à preservação do sigilo e da segurança; compatibilidade entre as políticas de segurança da informação e comunicações efetuadas pelos órgãos e entidades, no âmbito das atividades relativas ao compartilhamento de dados; a escolha e aprovação das bases temáticas a serem integradas ao CBC, com definição do cronograma de integração, em comum acordo com os gestores de dados; a solução de controvérsias no compartilhamento de dados entre os órgãos e entidades públicas federais solicitantes de dados e o gestor de dados.

Destaca-se que, no momento da impugnação da norma perante o STF, o CCGD era composto por representantes dos seguintes órgãos e entidades: dois do Ministério da Economia (dentre os quais um da Secretaria Especial de Desburocratização, Gestão e Governo Digital, que o presidiria, e um da Secretaria Especial da Receita Federal do Brasil); um da Casa Civil da Presidência da República; um da Secretaria de Transparência e Prevenção da Corrupção da Controladoria-Geral da União (CGU); um da Secretaria Especial de Modernização do Estado da Secretaria-Geral da Presidência da República; um da Advocacia-Geral da União (AGU); e um do Instituto Nacional do Seguro Social (INSS). Os membros eram indicados pelos titulares dos órgãos ou d entidade que representam e designados pelo Ministro da Economia, sendo que o quórum das reuniões era de dois terços de seus membros, ao passo que as aprovações eram por consenso.

Por último, o quinto eixo consiste nas disposições finais e transitórias.

2. A AÇÃO DIRETA DE INCONSTITUCIONALIDADE N.º 6.649

Feita a apresentação da norma federal impugnada, adentra-se no exame da ADI n.º 6.649.

A ADI n.º 6.649 foi proposta em dezembro de 2020 pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) em face do Decreto Federal n.º 10.046, de 2019, na redação dada pelo Decreto n.º 10.332, de 2020. Ingressaram como *amici curiae* na demanda, reforçando os fundamentos do CFOAB, a Associação *Data Privacy* Brasil de Pesquisa, o Laboratório de Políticas Públicas e Internet (LAPIN) em parceria com a Coalização de Direitos na Rede (CDR) e o Instituto Mais Cidadania.

Os atores que propugnaram pela inconstitucionalidade da norma (doravante referidos como "requerentes" ou "postulantes") afirmaram a ocorrência de violação aos artigos: 84, incisos IV e VI, alínea "a"; 1º, *caput*, inciso III; e 5º, *caput*, e *incisos* X, XII e LXXII da Constituição Federal[9]. Seus argumentos, afastados os apontamentos de índole processual e de inconstitucionalidade formal, podem ser congregados em três principais[10], expostos a seguir, juntamente com os correspondentes contra-argumentos da Administração Pública Federal, a qual, a seu turno, defendeu a plena constitucionalidade do Decreto[11].

2.1. Os argumentos "em jogo" na ADI 6.649

a) (Possível) Violação dos direitos à proteção de dados pessoais e autodeterminação informativa

Sob a perspectiva material, o CFOAB e os *amici curiae* sustentaram que o Decreto impugnado violaria: a dignidade da pessoa humana; a inviolabilidade da intimidade, da privacidade, da honra e da imagem das pessoas; o sigilo dos dados; a garantia do *habeas data*; e os direitos à proteção de dados pessoais e à autodeterminação informativa[12]. No que tange especificamente aos últimos dois direitos, os atores envolvidos explicaram que, paulatinamente, foi sendo construída a autonomia deles frente ao direito fundamental à privacidade, o que teria, inclusive, sido reconhecido em âmbito nacional pelo STF no julgamento da ADI n.º 6.387.

De fato, diferentemente da concepção tradicional de privacidade (concebida como "o direito de ser deixado só"), os direitos à proteção de dados pessoais e à autodeterminação informativa foram atrelados à liberdade do indivíduo de autonomamente desenvolver sua personalidade, protegendo-se de medidas que, em um cenário de evolução tecnológica, poderiam miná-la, a exemplo do levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais[13].

9 À época, ainda não havia sido aprovada a Emenda Constitucional n.º 115, de 2022, que acresceu ao rol do artigo 5º da Constituição Federal o "(...) direito à proteção de dados pessoais, inclusive nos meios digitais" (inciso LXXIX).

10 Para a definição desses fundamentos, promoveu-se um estudo da petição inicial da ADI 6.649 e das peças de manifestações dos *amici curiae*, com correspondentes anexos, conforme autos públicos digitais disponíveis no sítio eletrônico do Supremo Tribunal Federal.

11 Os argumentos da Administração Pública Federal foram extraídos da Nota Técnica SEI n.º 5901/2020/ME, da Nota SAJ nº 4/2021/CGIP/SAJ/SG/PR, do Parecer n. 00009/2021/PGFN/AGU, das Informações n. 00008/2021/CONSUNIAO/CGU/AGU e da peça de defesa da AGU, conforme autos públicos digitais disponíveis no sítio eletrônico do Supremo Tribunal Federal.

12 Para uma exposição sobre a relação entre os direitos aventados e o direito fundamental à proteção de dados pessoais, vide: MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

13 O marco para o reconhecimento do direito fundamental à proteção de dados pessoais e à autodeterminação informativa foi a decisão do Tribunal Constitucional Alemão de 1983, relativa à Lei do Recenseamento. Para maiores detalhes sobre a decisão, vide: HORNUNG, Gerrit e SCHNABEL, Christoph. Data protection in Germany I: The population census decision and the right to informational self-determination. Elsevier Ltd: Computer law & security review 25 (2009), pp. 84–88.

É que, com o processamento eletrônico de dados, tornou-se possível que informações detalhadas de um indivíduo sejam ilimitadamente armazenadas e rapidamente consultadas, de qualquer distância, de modo a estruturar um perfil de personalidade apurado, sem que a pessoa atingida tenha conhecimento ou mesmo controle de como tais informações serão utilizadas ou para quem serão transmitidas. Isso prejudicaria o livre arbítrio do indivíduo (base estruturante do Estado Democrático), pois a pessoa que não conseguiria determinar, com segurança, quais informações sobre si são conhecidas, de forma que poderia ser inibida em sua liberdade de planejar e decidir com autodeterminação.

Portanto, a autodeterminação informativa e a proteção de dados pessoais buscam resguardar os direitos do titular dos dados de (i) ser protegido dos riscos que o tratamento de dados gera ao desenvolvimento da sua personalidade e (ii) ter controle e gestão sobre suas próprias informações. Nessa toada, ao longo dos anos, foram extraídos desses direitos um conjunto de princípios capazes de auxiliar na verificação da legitimidade de determinado tratamento de dados[14]. Merecem destaque, no propósito de compreender os argumentos em jogo na ADI 6.649, os seguintes, apresentados conforme definição extraída do artigo 6º da LGPD:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; (...)
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

Na visão dos postulantes, o Decreto n.º 10.046 de 2019 violaria os direitos fundamentais indicados no início deste Tópico, por inobservância aos princípios da finalidade, adequação, necessidade, livre acesso e transparência.

Os princípios da **finalidade** e da **adequação** seriam desrespeitados, porque o Decreto não apregoaria a necessidade de o órgão receptor dos dados explicitar para qual finalidade eles serão utilizados; tampouco imporia uma restrição do uso ao contexto finalístico em que coletados. Em complemento, afirmou-se que os objetivos de compartilhamento insculpidos no artigo 1º do Decreto seriam excessivamente amplos, possibilitando uma distorção para fins de maximização incontrolável na coleta e no tratamento dos dados.

Igualmente, seria violado o princípio da **necessidade**, na medida em que o Decreto fomentaria a coleta e o uso excessivo de dados pessoais. Ressaltou-se, nesse particular, a previsão, como dados coletáveis, de alguns dados não mencionados na LGPD, como "fatos da vida", na categoria de atributos biográficos, e "a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar", na categoria de atributos biométricos.

Os princípios do **livre acesso** e da **transparência**, ainda no entendimento dos requerentes, seriam descumpridos pela falta de mecanismos para que os titulares dos dados tivessem conhecimento

14 Para maiores detalhes sobre os princípios de proteção de dados pessoais, ver: DONEDA, Danilo. Princípios de proteção e dados pessoais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). Direito e Internet III: Marco Civil da Internet (Lei n. 12.965/2014). Tomo I. São Paulo: Quartier Latin, 2015, pp. 369-384.

do fluxo de seus dados pessoais entre os órgãos da Administração Pública, bem como pela inexistência de previsão na normativa quanto ao exercício de direitos para acesso, conferência e retificação dos dados pessoais pelos titulares. Acrescentou-se crítica sobre a desnecessidade de formalização de instrumentos jurídicos para o compartilhamento de dados (artigo 5º do Decreto), sob o fundamento de que justamente por meio desses instrumentos é que se poderiam oferecer informações objetivas sobre a atividade de tratamento de dados (escopo, finalidade e, inclusive, a responsabilidade de cada controlador).

Outro aspecto do Decreto censurado pelos postulantes foi a categorização dos compartilhamentos de dados a partir do critério do sigilo ou não do dado. Nesse tocante, frisou-se que, mesmo que dados pessoais que tenham sido publicizados para uma dada finalidade, seria necessário observar os princípios da LGPD para que eles fossem utilizados em outros contextos.

Em contraposição aos postulantes, a Administração Pública Federal argumentou que o Decreto, por diversas vezes, fez remissão aos preceitos da LGPD, guardando, pois, compatibilidade com a legislação protetiva de dados pessoais. No mais, alegou que o Decreto não autorizaria a divulgação ou compartilhamento dos dados sem critérios. Ao contrário, quando um dado custodiado pela Administração fosse enquadrado no nível de categoria mais rígida ("compartilhamento específico"), tal dado necessitaria de autorização específica, a partir de um pedido devidamente justificado para poder ser compartilhado, ainda que dentro da própria Administração.

Aqui, para maior elucidação, cumpre mencionar a narrativa da União de que o CBC corresponderia à base cadastral do CPF da Receita Federal e que, ao longo do ano de 2020, o acesso a esses dados teria sido disponibilizado aos órgãos federais por meio de um contrato centralizado com as empresas públicas SERPRO e DATAPREV, aos quais as unidades administrativas precisariam aderir. Todavia, para aderir a esse contrato centralizado, o órgão precisaria, antes, solicitar autorização expressa à Receita Federal, justificando a finalidade do acesso (que teria de ser para execução de políticas públicas) e se comprometendo com os requisitos de segurança da informação e proteção de dados pessoais. Somente após a autorização da Receita é que os dados seriam disponibilizados para os órgãos.

Na mesma linha de raciocínio, aduziu que a utilização dos termos genéricos "políticas públicas" ou "serviços públicos" no bojo do Decreto para aludir às justificativas para o compartilhamento decorreria simplesmente da impossibilidade de prever, *a priori*, a totalidade dos serviços que serão demandados pela sociedade. O uso desses termos genéricos, inclusive, também ocorreria na LGPD.

Além disso, a União alegou que o Decreto preservou direitos e garantias fundamentais, porquanto, além de limitada exclusivamente ao setor público, a forma de compartilhamento de dados por ele assimilada: (i) não englobaria informações protegidas por sigilo fiscal; (ii) observaria as restrições legais, os requisitos de segurança da informação e o disposto na LGPD; (iii) sujeitaria o recebedor de dados sigilosos aos mesmos deveres impostos ao custodiante; (iii) ressalvaria, expressamente, o direito à preservação da intimidade e da privacidade da pessoa natural; e (iv) seria permitida pelo artigo 11, inciso II, alínea "b", da LGPD, que autoriza o tratamento de dados pessoais para as finalidades indicadas, inclusive nos casos de dados sensíveis, sem a necessidade de autorização expressa por parte de seu titular.

b) (Possível) Ausência de proporcionalidade na instituição do Cadastro Base do Cidadão

O autor da ADI e os *amici curiae* contestaram a proporcionalidade da criação do CBC face aos direitos à proteção de dados pessoais e à autodeterminação informativa.

De um lado, obtemperaram que a criação de uma base extensa de dados traria instrumentos para que o Estado exercesse vigilância excessiva, controle e manipulação dos cidadãos, inclusive para eventuais propósitos políticos e discriminatórios. Nessa ordem de ideias, narraram as experiências de Alemanha, Estados Unidos e França, países que, seja mediante atuação parlamentar, seja por decisão judicial, rechaçaram propostas de criação de grandes bancos de dados estatais.

De outro, foram externadas preocupações com riscos de vazamento de dados associados ao CBC. Segundo os requerentes, os mecanismos de interoperabilidade da base integradora com as bases de dados temáticas fariam com que existissem diversos pontos de vulnerabilidade passíveis de serem explorados por sujeitos mal-intencionados. Afinal, caso se encontrasse falhas de segurança no sistema de um único órgão, seria possível acessar informações em bases de muitos outros.

Em complemento, os postulantes sugeriram que as disposições do Decreto sobre segurança da informação seriam genéricas e com teor essencialmente programático, não havendo sequer referência à elaboração de uma avaliação de impacto, nos termos do artigo 38 da LGPD, previamente à operação do CBC. Aludiu-se, ainda, à ausência de mecanismos de prestação de contas e de responsabilização de agentes públicos por desvios no tratamento de dados, o que se agravaria pelo fato de a figura do "gestor de dados", criada pelo Decreto, não ser equivalente à do "encarregado" presente na LGPD, de forma que não estaria claro se os deveres e responsabilidades deste último seriam aplicáveis ao primeiro.

Em suma, concluíram afirmando que a criação do CBC não se sustentaria pelo crivo da proporcionalidade, consideradas as subregras da adequação, necessidade e proporcionalidade em sentido estrito. No seu entendimento, o ato normativo objeto da ADI seria inadequado, pois não apresentaria justificativa satisfatória a embasar a criação de uma gigantesca base de dados dos cidadãos; não seria necessário, eis que o acesso compartilhado, sem delimitações específicas, extrapolaria o necessário para atuação governamental; e seria desproporcional, na medida em que os riscos aos direitos fundamentais dos cidadãos superariam as vantagens da criação do CBC, ante a falta de previsão de mecanismos suficientes à proteção dos titulares e por possibilitar o uso excessivo dos seus dados.

Noutro giro, a União buscou salvaguardar o CBC, afirmando a inexistência de finalidades ilícitas no compartilhamento técnico dos dados. Nessa direção, a fim de contestar o argumento sobre a criação de uma base massiva de dados dos cidadãos, asseverou que o CBC, por si, não geraria, copiaria ou duplicaria nenhum dado, mas, sim, possuiria mecanismos de consulta dos dados, em tempo real, nas bases já existentes em órgãos do governo, para a finalidade exclusiva de oferta de serviços e de gestão de políticas públicas.

Além disso, a Administração caracterizou o CBC como manifestação da eficiência administrativa em prol do cidadão. Sob essa perspectiva, enfatizou que o CBC seria um mecanismo essencial para a autenticação digital, que, por sua vez: reduziria a ocorrência de falsificação ideológica e duplicação de identificação, evitando fraudes e estelionatos; traria maior confiabilidade às operações, inclusive transa-

ções financeiras; simplificaria e automatizaria procedimentos de prova de vida e identificação, reduzindo custos e riscos no fornecimento de serviços públicos. Frisou-se, outrossim, a importância do CBC para evitar informações contraditórias que impossibilitariam o acesso dos cidadãos a programas sociais ou, ainda, que implicariam a concessão de benefícios a pessoas não habilitadas a recebê-los.

No mais, disse que, com a criação do CBC, o Executivo federal teria adotado o mesmo princípio da União Europeia para proteção de dados pessoais, qual seja, o princípio segundo o qual dados particulares devem ser apresentados somente uma vez ao Poder Público na prestação de serviços variados (*Once-Only Principle*). O objetivo seria reduzir o fardo administrativo sobre pessoas físicas e jurídicas na obtenção de bens e serviços públicos, diminuindo a presença física do cidadão no órgão que presta serviços, bem como reduzindo ou eliminando o fornecimento de documentos de identificação já acessíveis pelo governo.

Ressaltou-se, também, que o compartilhamento possibilitaria a redução de custos de acesso, inclusive mediante o reaproveitamento de recursos de infraestrutura. A título de exemplo, apontou-se que a adesão de unidades administrativas federais ao contrato centralizado para lograr acesso ao CBC no ano de 2020 teria permitido o ajuste de cerca de trezentos serviços públicos para obter as informações biográficas de maneira automática, evitando que o cidadão precisasse reapresentar ao governo informações que este já possui e, ainda, que o governo as validasse manualmente. Segundo consta na Nota Técnica SEI nº 59061/2020/ME, as integrações em questão teriam trazido uma economia estimada de R$ 420 milhões[15].

Quanto à temática da segurança, apontou-se que bastaria uma leitura do inciso I do artigo 3º do Decreto para se atestar o alinhamento do Decreto nº 10.046, de 2019 à LGPD. Isso porque, ali, se determina que o compartilhamento de dados observe as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na LGPD. O artigo 7º ainda aprofundaria a proteção, ao determinar que as plataformas de interoperabilidade contemplem requisitos de sigilo, confidencialidade, gestão, auditabilidade e segurança da informação necessários ao compartilhamento de dados.

Prosseguindo, arguiu-se que o risco que paira sobre toda atividade administrativa não autorizaria a paralisia estatal e que o Estado brasileiro estava buscando aprimorar seus mecanismos de segurança da informação de caráter administrativo e técnico. Advertiu-se que o risco de uma exposição de dados que possa violar o direito à privacidade seria uma realidade, independentemente da edição do Decreto n. 10.046, de 2019, uma vez que as informações já se encontrariam fragmentadas em diversas bases de dados.

De toda forma, alegou-se que o Decreto teria atribuído ao CCGD a responsabilidade por traçar uma visão de futuro para a sustentação do CBC, além de assegurar que as deliberações estejam alinhadas às expectativas da sociedade, bem como às normas se existentes. Nessa óptica, a instituição do CCGD ajudaria a concretizar os preceitos fundamentais apontados pelo autor como violados, ampliando a transparência e a segurança na governança de dados e na gestão de informações sigilosas.

Em relação à responsabilização e à prestação de contas, destacou-se que a legislação em vigor já disporia de regras administrativo-disciplinares e criminais para punir as autoridades públicas que cometam excessos ou desvios de finalidade, no que concerne ao uso indevido de dados e informações pessoais. Não bastasse isso, a Administração Pública Federal teria de prestar contas à Autoridade Nacional de Proteção de Dados (ANPD) sobre suas atividades de proteção de dados pessoais.

15 Item 61 da mencionada Nota Técnica.

A União, pois, aduziu que a instituição do CDC observaria a proporcionalidade, tendo em vista: a presença de adequação entre o meio e a finalidade, pois o modelo de governança no compartilhamento de dados no âmbito da Administração Pública federal, além de possuir respaldo normativo, teria por objetivo imprimir maior eficiência à prestação dos serviços públicos e à gestão de políticas públicas; o meio empregado para o alcance dos referidos fins não poderia ser substituído por outro de natureza menos gravosa, tendo-se em vista que, para se continuar ofertando políticas e serviços públicos, mediante uso racional de recursos financeiros, seriam necessários mecanismos de qualificação e interoperabilidade segura entre as bases de dados que informem um processo de governança amplo e eficaz; e os benefícios advindos da medida caracterizariam sua proporcionalidade em sentido estrito, eis que possibilitariam maior celeridade e correção na prestação de políticas e serviços públicos.

c) (Possível) Inadequação da composição do Comitê Central de Governança de Dados

O último argumento que comporta referência concerne à composição do CCGD. Para os requerentes, seria problemático que o Comitê apenas possuísse integrantes da Administração Pública, mormente porque as experiências brasileira e internacional denotariam que, em questões relacionadas à tecnologia, o multissetorialismo seria a melhor prática.

A Administração Federal rebateu, argumentando que os membros do CCGD adviriam de órgãos com naturezas diferentes e complementares, exatamente para que os assuntos sob deliberação pudessem ser discutidos e amadurecidos: (i) a presença da AGU traria análises jurídicas para as decisões do Comitê; (ii) a CGU seria um órgão com atribuições de controle interno e transparência; (iii) a Receita Federal e o INSS possuiriam ampla maturidade em governança de dados e gestão de sigilo; (iv) e a Casa Civil, a Secretaria Especial de Modernização do Estado e a Secretaria Especial de Desburocratização, Gestão e Governo Digital contariam com uma visão abrangente das necessidades dos órgãos públicos, por desempenharem funções de articulação.

Outro ponto alegado foi que o Decreto prevê que qualquer membro do CCGD pode convidar especialistas para participar de suas reuniões e, com isso, trazer uma *expertise* multisetorial, ainda que sem direito a voto, para enriquecer os debates. No mais, asseverou-se que as decisões do Comitê seriam tomadas por consenso e divulgadas para a sociedade por meio do sítio eletrônico do CCGD e do Diário Oficial da União.

2.2. O voto vencedor

A ADI n.º 6.649 foi submetida à relatoria do Ministro Gilmar Mendes, cujo voto prevaleceu, por maioria, ao final do julgamento. Assim, o Supremo Tribunal Federal conheceu da ação e julgou os pedidos parcialmente procedentes, para fins de conferir interpretação conforme ao Decreto n.º 10.046, de 2019. Passa-se, adiante, à exposição dos principais fundamentos do voto vencedor[16], em diálogo com os três argumentos apresentados no Tópico 3.1., supra.

No que toca à alegação mais substanciosa de **violação a princípios nucleares dos direitos à proteção de dados pessoais e à autodeterminação informativa (a)**, o Ministro Gilmar Mendes desen-

16 Houve o julgamento conjunto da ADI 6.649 e da ADPF 695. Porém, em atenção aos objetivos deste artigo, a exposição centrar-se-á essencialmente nos aspectos pertinentes à análise da constitucionalidade do Decreto n.º 10.046, de 2019.

volveu um interessante raciocínio de interpretação conforme, que comporta explicação mais detalhada.

Nos termos do voto vencedor, o Decreto n.º 10.046, de 2019 seria o resultado de uma busca por sistematizar regras, para fins de aplicação harmônica da Lei de Acesso à Informação (LAI) e da LGPD, as quais possuem matizes distintas. Essa distinção imporia um regime jurídico híbrido para o tratamento das informações coletadas ou produzidas pela Administração Pública, a depender do maior ou menor vínculo que elas guardem com os atributos da personalidade ou com qualidades próprias do cidadão.

Para as informações gerais do Estado (relativas ao funcionamento do aparato estatal, como gestão de pessoal e patrimônio público, utilização de recursos orçamentários, formalização de atos e contratos etc.), vigoraria um regime flexível, norteado pelo acesso à informação e pelo controle da atividade estatal.

Destarte, quando o artigo 3º, inciso I, do Decreto diz que: "a informação do Estado será compartilhada da forma mais ampla possível (...)", deve-se interpretar que apenas as informações gerais do Estado estariam abrangidas. Na mesma vertente deveriam ser compreendidas as normas que impõem ampla divulgação, preferencialmente em canais de dados abertos e de transparência ativa, de informações públicas (artigo 4º, inciso I, que versa sobre o "compartilhamento amplo"); e as que aludem ao compartilhamento limitado de informações sigilosas do Estado (artigos 4º, incisos II e III, que dispõem sobre os compartilhamentos "restrito" e "específico").

Noutro giro, as informações pessoais dos cidadãos estariam submetidas aos vetores mais rigorosos da LGPD, que estatuem a necessidade do preenchimento de requisitos rígidos para o fluxo de informações no âmbito dos órgãos públicos federais. E, nesse particular, o Ministro salientou que, como o Decreto, em diversos pontos, faz remissões às regras e aos princípios da LGPD, ele não conteria qualquer permissão para que o compartilhamento de dados pessoais entre órgãos e entidades federais ocorresse de maneira irrestrita.

Portanto, no intuito de afastar qualquer dúvida interpretativa, o Relator estabeleceu, na conclusão de seu voto, as seguintes balizas de interpretação conforme para o Decreto Federal n.º 10.046, de 2019 nesse tocante:

> 1. O compartilhamento de **dados pessoais** entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de **propósitos legítimos, específicos e explícitos** para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) **compatibilidade** do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao **mínimo necessário** para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, 'no que for compatível com o setor público'. (...)
>
> 2. O compartilhamento de **dados pessoais** entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental **compartilha ou tem acesso** a banco de dados pessoais, 'fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.' (destaques no original)

A mesma linha de intelecção foi adotada no voto vencedor no que tange à **proporcionalidade da instituição do Cadastro Base do Cidadão (b).** É que, para o Ministro Relator, desde que interpretados em conformidade com a LGPD, os preceitos do Decreto não abririam espaço para a instituição de uma base integradora massiva, porquanto o regime protetivo da LGPD – em especial seus artigos 6º, 7º e 23 – traria

a necessidade de estabelecimento de ferramentas rigorosas de controle de acesso ao CBC.

Não somente, o Relator expressou que a violação ao direito à proteção de dados traria ao cidadão a possibilidade de reparação civil frente ao Estado, o qual, a seu turno, teria direito de regresso face ao servidor nos casos de dolo ou culpa. Em complemento, o servidor infrator também estaria sujeito a punições disciplinares e por improbidade administrativa.

A solução foi igualmente objeto de interpretação conforme na conclusão do voto:

> 3. O acesso de órgãos e entidades governamentais ao Cadastro Base do Cidadão fica condicionado ao atendimento integral das diretrizes acima arroladas, cabendo ao Comitê Central de Governança de Dados, no exercício das competências aludidas nos arts. 21, incisos VI, VII e VIII do Decreto 10.046/2019:
>
> 3.1. prever mecanismos rigorosos de controle de acesso ao Cadastro Base do Cidadão, o qual será limitado a órgãos e entidades que comprovarem **real necessidade** de acesso aos dados pessoais nele reunidos. Nesse sentido, a permissão de acesso somente poderá ser concedida para o alcance de propósitos legítimos, específicos e explícitos, sendo limitada a informações que sejam indispensáveis ao atendimento do interesse público, nos termos do art. 7º, inciso III, e art. 23, caput e inciso I, da Lei 13.709/2018;
>
> 3.2. justificar prévia e minudentemente, à luz dos postulados da proporcionalidade, da razoabilidade e dos princípios gerais de proteção da LGPD, tanto a necessidade de inclusão de novos dados pessoais na base integradora (art. 21, inciso VII) como a escolha das bases temáticas que comporão o Cadastro Base do Cidadão (art. 21, inciso VIII).
>
> 3.3. instituir medidas de segurança compatíveis com os princípios de proteção da LGPD, em especial a criação de sistema eletrônico de registro de acesso, para efeito de responsabilização em caso de abuso.
>
> (...)
>
> 5. O tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei 13.709/2018, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de culpa ou dolo.
>
> 6. A transgressão dolosa ao dever de publicidade estabelecido no art. 23, inciso I, da LGPD, fora das hipóteses constitucionais de sigilo, importará a responsabilização do agente estatal por ato de improbidade administrativa, nos termos do art. 11, inciso IV, da Lei 8.429/92, sem prejuízo da aplicação das sanções disciplinares previstas nos estatutos dos servidores públicos federais, municipais e estaduais.

Quanto ao argumento pertinente à **inadequação do desenho institucional do CCGD (c)**, este foi reputado procedente no voto vencedor. O Relator argumentou pela existência de consenso em torno da necessidade de, no âmbito de atividades pertinentes ao direito à privacidade, criar autoridades administrativas independentes, destacadas especificamente para a fiscalização e controle de atividades potencialmente lesivas. Citou, para corroborar sua afirmação, a experiência de países democráticos estrangeiros e a experiência setorial brasileira – notadamente na ANPD e no Comitê Gestor do Programa de Identificação Civil Nacional, da Lei n.º 13.444, de 2017.

O Ministro consignou, portanto, a inconstitucionalidade da instituição do CCGD com composição exclusiva por representantes dos Poder Executivo, sem quaisquer garantias contra influências indevidas. Contudo, no intuito de não gerar demasiados prejuízos com a desestruturação da entidade responsável pelo estabelecimento de limites ao compartilhamento de dados entre órgãos da Administração Federal, o Relator conferiu efeitos prospectivos à declaração de inconstitucionalidade da composição do CCGD, mantendo estrutura do Comitê por mais sessenta dias, prazo hábil para que fosse atribuído ao órgão um perfil independente e plural, aberto à participação efetiva de representan-

tes de outras instituições democráticas, conferindo-se aos seus integrantes garantias mínimas contra influências indevidas.

3. PRINCIPAIS REFLEXOS NORMATIVOS DO JULGAMENTO

O julgamento da ADI 6.649 trouxe nítidos impactos para o regime normativo de compartilhamento de dados na Administração Pública federal. Isso porque, cerca de dois meses após a publicação da ata do julgamento, foi publicado o Decreto Federal n.º 11.226, de 2022, que promoveu alterações no Decreto n.º 10.046, de 2019, sendo que o conteúdo da norma modificadora denota uma busca pela observância aos parâmetros colocados pelo STF[17].

Em relação aos **princípios derivados dos direitos à proteção de dados pessoais e à autodeterminação informativa (a)**, constata-se que o item 1 da parte dispositiva do voto do vencedor, que alude ao conteúdo dos princípios da finalidade, adequação e necessidade para o compartilhamento de dados pessoais entre órgãos e entidades da Administração Federal, foi incluído no bojo das diretrizes de compartilhamento insculpidas no artigo 3º do Decreto (incisos VII a IX). De forma semelhante, o item 2 da parte dispositiva do voto, referente à necessidade de publicidade e transparência no mencionado compartilhamento, foi contemplado nos parágrafos 1º e 2º do artigo 5º do Decreto.

Além disso, estabeleceu-se no § 3º do artigo 5º do Decreto que o compartilhamento de dados nos níveis restrito e específicos serão autorizados pelo gestor de dados e seu processo será formalizado por documentos de interoperabilidade cuja solicitação seguirá os critérios estabelecidos pelo CCGD, em observância à LGPD, à Lei do Governo Digital (Lei n.º 14.129, de 2021), à LAI, às orientações da ANPD e às normas correlatas. Aqui, também se acrescentou o § 4º no mesmo artigo 5º, para reforçar que as operações de interoperabilidade que envolvam dados pessoais deverão, também, explicitar: (i) propósito legítimo, específico e explícito; (ii) compatibilidade com a finalidade; e (iii) o compartilhamento mínimo necessário para o atendimento da finalidade.

No que tange ao **Cadastro Base do Cidadão (b)**, a observância do item 3.1. da parte dispositiva do voto, relativa à restrição do acesso ao CBC, deu-se a partir da expressa previsão no artigo 17, § 2º, de que o acesso dos órgãos e das entidades ao CBC deve observar as diretrizes de finalidade, adequação e necessidade. Em complemento, por meio da inclusão do § 3º no artigo 17, previu-se a responsabilidade do CCGD por estabelecer mecanismos de controle de acesso ao CBC, o qual será limitado a órgãos e entidades que comprovarem real necessidade de acesso aos dados pessoais nele reunidos.

Quanto aos itens 3.2. e 3.3. da parte dispositiva do voto, concernentes à necessidade de justificativa prévia para a inclusão novos dados na base integradora e instituição de sistemas eletrônicos de registro de acesso ao CBC para fins de responsabilização em caso de abuso, esses foram previstos no artigo 17, § 7º e 20-A do Decreto, respectivamente. No mais, foi incluído o artigo 15-A na norma, explicitando-se que os danos causados pelos órgãos e entidades federais no tratamento de dados pessoais importariam em responsabilidade civil do Estado, com possibilidade de regresso contra os agentes públicos responsáveis,

17 Observe-se que o Decreto Federal n.º 10.049, de 2019 foi modificado recentemente pelo Decreto Federal n.º 11.574, de 2023, especialmente no que tange a alguns órgãos responsáveis pelas atividades delimitadas no Decreto, o que se associa ao advento de uma nova gestão no Governo Federal em 2023. A exposição feita no artigo contempla as novidades do novel Decreto.

em casos de dolo ou culpa.

Prosseguindo, houve alteração do **desenho institucional do CCGD (c)**, previsto nos artigos 22 a 25 do Decreto n.º 10.046. Adiante, será feita a explicitação de tais mudanças já considerando a redação dada pelo novel Decreto n.º 11.574, de 2023.

Em relação à composição original, foram promovidas as seguintes distinções: (i) em vez de um membro Secretaria Especial de Desburocratização, Gestão e Governo Digital, colocou-se um representante do órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação - Sisp, que presidirá o CCGD; (ii) substitui-se o representante do INSS por um do Ministério da Previdência Social e um do Ministério do Trabalho e Emprego; (iii) não mais se especificou que o representante da CGU deve provir da Secretaria de Transparência e Prevenção da Corrupção; (iv) deixou-se de prever a participação de um representante da Secretaria Especial de Modernização do Estado; e (v) incluiu-se um representante um do Ministério da Justiça e Segurança Pública e dois de organizações da sociedade com atuação comprovada na temática de proteção de dados pessoais.

Previu-se que os dois membros oriundos de organizações da sociedade serão selecionados mediante processo seletivo, conforme regulamento editado pelo CCGD, e terão mandato de dois anos, permitida uma recondução. Ademais, eles terão direito a voto nas deliberações relativas à gestão de tratamento de dados pessoais. Os demais integrantes obrigatórios serão indicados pelos órgãos que representam e designados em ato do Secretário de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos.

Além dos membros obrigatórios, estatuiu-se a possibilidade de que o CCGD contenha membros convidados, notadamente: um do Conselho Nacional de Justiça, um do Senado Federal e um da Câmara dos Deputados. A indicação desses membros convidados constitui ato discricionário dos órgãos representados e, havendo indicação, eles terão direito a voto nas deliberações relativas à gestão de dados pessoais.

Outrossim, houve alteração dos quóruns: o de reunião passou a ser de dois terços dos membros, ao passo que o de aprovação passou a ser de maioria simples.

4. CONSIDERAÇÕES FINAIS

A partir da detida análise da ADI n.º 6.649, há como se extrair, principalmente do voto vencedor do Ministro Gilmar Mendes, alguns parâmetros abstratos para o compartilhamento de dados no âmbito da Administração Pública, tais como:

> (i) Os dados coletados e armazenados pela Administração Pública se submetem a um regime híbrido: os pertinentes à atividade administrativa do Estado se sujeitam a um regime mais flexível, próprio da LAI, de modo que seu fluxo entre os diversos órgãos e entidades está associado ao grau de sigilo do dado; porém, os dados pessoais dos cidadãos se submetem ao regime da LGPD para tratamento de dados pelo Poder Público, inclusive no que diz respeito à observância de princípios derivados do direito à proteção de dados, como finalidade, adequação, necessidade e transparência;
>
> (ii) A criação de uma base integradora de dados de outras bases temáticas, como o Cadastro Base do Cidadão, não é, em si, inconstitucional, mas deve ser permeada pela adoção de cautelas quando envolver dados pessoais dos cidadãos, dentre as quais: a restrição do acesso apenas àqueles órgãos que demonstrarem real necessidade, a exigência de justificativa explícita para o acréscimo de dados na base integradora e a existência de mecanismos de registro de acesso, para fins de responsabilização por eventuais abusos; e

> (iii) O órgão central que estabelece diretrizes e fiscaliza o compartilhamento deve ter uma composição plural, que inclua instituições externas à Administração Pública, e seus membros devem ter asseguradas garantias mínimas contra influências indevidas.

Ocorre que o atendimento a tais parâmetros admite uma série de distintas conformações normativas. E, no caso específico da Administração Pública Federal, a concretização desses preceitos dependerá, em essência, da atuação do CCGD. É que as modificações introduzidas no Decreto n.º 10.046, de 2019 pelo Decreto n.º 11.266, de 2022 não avançaram para além da reprodução dos amplos preceitos da decisão do STF, e, com isso, atribuíram a responsabilidade por sua efetivação principalmente ao CCGD. Nessa direção, pode-se citar, exemplificativamente, a fixação de critérios para as solicitações de compartilhamento nos níveis de compartilhamento restrito e específico (artigo 5º, § 3º); o estabelecimento de mecanismos de controle de acesso ao CBC (art. 17, § 3º); a instituição de medidas de segurança compatíveis com os princípios previstos na LGPD (artigo 20-A).

Prosseguindo, o estudo conjunto dos autos da ADI n.º 6.649 e da atual redação do Decreto Federal n.º 10.046, de 2019 permite aferir que determinados temas ficaram pendentes de equacionamento. Possivelmente o mais importante deles se relaciona aos riscos de vulnerabilidades de segurança do CBC, aspecto que foi amplamente desenvolvido pelos postulantes da ADI, mas ao qual não foi conferido peso argumentativo no voto do relator; a questão tampouco ganhou concretude com as alterações do decreto, tornando-se também uma temática a ser enfrentada pelo CCGD, como dito supra.

Outro aspecto não solucionado é o da ausência de diálogo entre a figura do gestor de dados, prevista no Decreto, e as figuras da LGPD, como a do encarregado de dados. Esse fator gera dúvidas quanto à necessidade de existência das duas figuras e, em caso de coexistência, quanto às atribuições a serem desempenhadas por cada qual.

Por último, questão que comporta reflexão é se o desenho institucional agora conferido ao CCGD atende aos parâmetros estabelecidos pelo STF. É que, não obstante se tenha incluído na sua composição dois membros obrigatórios provenientes de organizações da sociedade, todos os demais integrantes obrigatórios advêm de órgãos da Administração Pública Federal, sendo que o quórum de aprovação das deliberações passou a ser de maioria simples, ou seja, ele pode ser alcançado apenas pelos votos dos representantes da Administração.

Note-se que essa composição não se equipara à de outros órgãos de proteção de dados existentes no Brasil. O Conselho Nacional de Proteção de Dados (disciplinado no artigo 58-A da LGPD), por exemplo, contém participação de representantes de diversos setores, como: Administração Pública, Legislativo, Judiciário, Ministério Público, entidades da sociedade civil, instituições científicas, confederações sindicais etc.

De mais a mais, à exceção do mandato de dois anos resguardado aos integrantes provenientes de organizações da sociedade, não se extrai do Decreto garantias contra influências indevidas.

REFERÊNCIAS BIBLIOGRÁFICAS

DONEDA, Danilo. **Princípios de proteção e dados pessoais**. In: DE LUCCA, Newton; SIMÃO FILHO,

Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). Direito e Internet III: Marco Civil da Internet (Lei n. 12.965/2014). Tomo I. São Paulo: Quartier Latin, 2015, pp. 369-384.

HORNUNG, Gerrit e SCHNABEL, Christoph. **Data protection in Germany I: The population census decision and the right to informational self-determination**. Elsevier Ltd. doi:10.1016/j.clsr.2008.11.002: Computer law & security review 25 (2009), pp. 84–88.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014.

PFEIFFER, Roberto Augusto Castellanos. **Direito da concorrência, plataformas digitais e dados pessoais.** Tese (concurso Livre-docente em direito comercial – Edital FD 08/2021). Faculdade de Direito da Universidade de São Paulo. São Paulo, 2021.

SUPREMO TRIBUNAL FEDERAL, **Ação Direta de Inconstitucionalidade nº 6.387/DF**, Relatora Ministra Rosa Weber, julgado 07.05.2020.

SUPREMO TRIBUNAL FEDERAL, **Suspensão de Liminar n.º 1.103, Medida Cautelar,** Relatora Ministra Carmen Lúcia, julgado em 05.02.2017.

SUPREMO TRIBUNAL FEDERAL, **Mandado de Segurança n.º 36.150**, Medida Cautelar, Relator Ministro Luís Roberto Barroso, julgado em 10.12.2018.

SUPREMO TRIBUNAL FEDERAL, **Ação de Descumprimento de Preceito Fundamental n.º 695 e Ação Direta de Inconstitucionalidade n.º 6.649**, Relator Ministro Gilmar Mendes, julgado em 15.09.2022.

WIMMER, Miriam. **Limites e possibilidade para o uso secundário de dados no Poder Público: Lições da Pandemia**. *In:* Revista Brasileira de Políticas Públicas. Vol. 11, n.º 1. Abr. 2021.